December 17, 2004

Information Technology

DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness (D-2005-025)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
17 DEC 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**46**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at http://www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms

ASD (NII)/CIO	Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer
DeCA	Defense Commissary Agency
DCMA	Defense Contract Management Agency
DISA	Defense Information Systems Agency
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers Financial Integrity Act
IA	Information Assurance
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
WHS	Washington Headquarters Service

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

December 17, 2004

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS
ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/CHIEF INFORMATION OFFICER

SUBJECT: Report on DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness (Report No. D-2005-025)

We are providing this report for review and comment. We considered management comments on a draft of this report in preparing the final report.

DoD Directive 7650.3 requires that all issues be resolved promptly. All the recommendations remain unresolved. Therefore, we request that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide comments on this final report by January 21, 2005.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to Audam@dodig.osd.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Kathryn M. Truex at (703) 604-8966 (DSN 664-8966) or Ms. Sarah Davis at (703) 604-9031 (DSN 664-9031). See Appendix D for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Kathryn M. Truex for

Mary L. Ugone
Assistant Inspector General
for Acquisition and Technology Management

Office of the Inspector General of the Department of Defense

Report No. D-2005-025 **December 17, 2004**
(Project No. D2004AL-0136)

DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness

Executive Summary

Who Should Read This Report and Why? The DoD Chief Information Officer, the Under Secretary of Defense for Personnel and Readiness, the Director of the Defense Information System Agency, and the Chief Information Officers of DoD Components should read this report to obtain information about DoD implementation of the Federal Information Security Management Act training requirements. This report discusses the overall ability of DoD to report reliable training information required by the Federal Information Security Management Act and the effectiveness of the process that three DoD Components used to develop the required training information.

Background. This report is in response to Federal Information System Management Act requirements. On December 17, 2002, the President signed the E-Government Act of 2002 (Public Law 107-347) that included title III, section 301, "Federal Information Security Management Act of 2002." The Federal Information Security Management Act provides a comprehensive framework for ensuring the effectiveness of information security controls, management, and oversight required to protect Federal information and information systems. The Federal Information Security Management Act directs each agency to develop, document, and implement an agencywide information security program and to report annually to the Director of the Office of the Management and Budget, congressional committees, and the General Accountability Office on the adequacy and effectiveness of its information security policies, procedures, and practices. In addition, the Federal Information Security Management Act requires the Inspectors General of each agency to perform an independent evaluation of the agency's information security programs and practices.

On August 23, 2004, the Office of Management and Budget issued Memorandum 04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," which included a set of questions for each agency and its Inspector General to answer as part of the Federal Information Security Management Act reporting process. Section G asked how many agency employees received security awareness training in FY 2004 and how many employees with significant information technology security responsibilities received specialized training.

Results. The DoD Chief Information Officer did not ensure that training information that the DoD Components reported in response to the Federal Information Security Management Act data calls was accurate and supportable. In particular, the DoD Chief Information Officer did not ensure that all DoD Components had appropriately defined and identified employees with significant information technology security responsibilities, developed training requirements for those information technology

security professionals, or established processes to identify and track training taken by those individuals. This conclusion is specifically illustrated by the result of our review of three DoD Components. As a result, the DoD response to the training portion of the Office of Management and Budget FY 2004 reporting instructions for the Federal Information Security Management Act may not accurately reflect DoD enterprisewide compliance with the Federal Information Security Management Act requirements. (finding A).

The DoD Chief Information Officer did not ensure that security awareness training information that the DoD Components reported in response to the Federal Information Security Management Act data calls was accurate and supportable. Specifically, the Chief Information Officer did not ensure that the DoD Components had effective processes in place to track and monitor completion of security awareness training requirements. Although the Defense Commissary Agency and Washington Headquarters Service had processes in place to ensure that new employees receive initial security awareness training, the Washington Headquarters Service was the only agency of the three reviewed that had a process to ensure that its network users were receiving the required periodic training. This condition occurred because the DoD Chief Information Officer had not established specific reporting mechanisms to monitor and oversee compliance with DoD Instruction 8500.2, "Information Assurance," by DoD Components. As a result, security awareness training information that the DoD reported in FY 2004 cannot be relied upon to accurately reflect DoD enterprisewide compliance with Federal Information Security Management Act requirements, and network users that have not received training could introduce security vulnerabilities into DoD networks (finding B). See the Findings section of the report for the detailed recommendations.

Management Comments. The Director, Defense Information Assurance Program either did not concur with the recommendations or stated that the recommendations were no longer applicable because the recommended actions had been completed. Specifically, the comments stated that employees with significant information technology security responsibilities are defined in Appendix AP1 of the Draft Manual DoD 8570.1-M. The comments also stated that US Code Title 10 assigns the Services specific responsibilities for equipping, training, and providing the forces. Additionally, the comments stated that the Assistant Secretary of Defense for Networks and Information Integration has been working with the Under Secretary of Defense of Personnel and Readiness to develop methodologies for DoD Components to identify information assurance positions and manage and track employee training and certification requirements. See the Findings section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Audit Response. The Director, Defense Information Assurance Program comments were nonresponsive to the recommendations. DoD Directive 8570.1 specifically requires the Assistant Secretary for Networks and Information Integration/DoD Chief Information Officer to develop and promulgate additional guidance relating to information assurance training, certification, and workforce management requirements. The Directive also states that personnel and manpower databases under Under Secretary of Defense for Personnel and Readiness authority capture and report requirements for information assurance training and certification. Additionally, the implementing manual for DoD Directive 8570.1 has not yet been issued; until such a manual is issued and complied with, the recommended actions will not be completed. Therefore, we request that the Assistant Secretary for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments by January 21, 2005.

Table of Contents

Background

Federal Information Security Management Act of 2002. On December 17, 2002, the President signed the E-Government Act of 2002 (Public Law 107-347) that included title III, section 301, "Federal Information Security Management Act of 2002." The Federal Information Security Management Act (FISMA) provides a comprehensive framework for ensuring the effectiveness of information security controls, management, and oversight required to protect Federal information and information systems. FISMA directs each agency to develop, document, and implement an agencywide information security program and to report annually to the Director of the Office of the Management and Budget (OMB), congressional committees, and the General Accountability Office on the adequacy and effectiveness of its information security policies, procedures, and practices. In addition, FISMA requires Inspectors General to perform an independent evaluation of the information security programs and practices of their agencies.

OMB Guidance and Reporting Instructions. OMB identified security training and awareness as one of six Governmentwide security weaknesses in its FY 2001 FISMA report to Congress and since then has required Federal agencies to report on security awareness and specialized training every year. On August 23, 2004, OMB issued Memorandum 04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," which included a set of questions that each agency and its Inspector General must answer as part of the FISMA reporting process. Section G asked how many agency employees received security awareness training in FY 2004 and how many employees with significant information technology (IT) security responsibilities received specialized training.

Evolution of Federal Training Requirements. FISMA requires security awareness training for all IT users and additional training for personnel with significant IT security responsibilities. A requirement for periodic training in computer security awareness has existed since the enactment of the Computer Security Act of 1987. The Computer Security Act also assigned the responsibility for developing standards and guidelines for Federal computer security training to the National Institute of Standards and Technology (NIST). In November 1989, NIST issued Special Publication 500-172, "Computer Security Training Guidelines," which provided a framework for determining the training needs of particular categories of employees. In January 1992, the Office of Personnel and Management issued a Federal Personnel regulation, "Employees Responsible for the Management or Use of Federal Computer Systems" which made the recommended NIST guidelines mandatory. In April 1998, NIST issued Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," which focused on the job functions, roles, and responsibilities of each individual, rather than on job titles. The new approach recognized that an individual may have more than one role in an organization and would need IT security training to satisfy the specific responsibilities of each role. In October 2003, NIST issued Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program," as a companion document to NIST 800-16. NIST 800-50 discusses how to build an IT security awareness and training program, and

NIST 800-16 describes an approach to role-based IT security training. For more information on NIST 800-50 and 800-16, see Appendix B.

Objectives

The overall audit objective was to assess DoD implementation of title III, section 301, "Federal Information Security Management Act," of the E-Government Act of 2002 (Public Law 107-347). Specifically, we evaluated whether all agency employees, including contractors, received IT security training and awareness and whether employees with significant IT security responsibilities were properly trained for their level of responsibility. See Appendix A for a discussion of the scope and methodology and prior coverage related to the objectives.

A. Specialized Training for Employees with Significant Security Responsibilities for Information Technology

The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (DoD CIO) did not ensure that training information that the DoD Components reported in response to FISMA data calls was accurate and supportable. In particular, the DoD CIO did not ensure that all DoD Components had appropriately defined and identified employees with significant IT security responsibilities, developed training and certification requirements for those IT security professionals, or established processes to track and monitor training taken by those individuals. This conclusion is specifically illustrated by the result of our review of three DoD Components. This condition occurred because the DoD CIO did not implement the requirements of numerous policy documents issued since 1998 and did not establish specific reporting mechanisms to monitor and oversee accomplishment of those requirements by DoD Components. Further, DoD did not consistently report on actions required to correct this ongoing enterprisewide deficiency. As a result, the DoD response to the training portion of the OMB FY 2004 reporting instructions for FISMA may not accurately reflect DoD enterprisewide compliance with FISMA requirements.

NIST Special Publication 800-50

OMB Memorandum 04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004, asks Federal agencies whether their employees with significant IT security responsibilities received specialized training as described in NIST Special Publications 800-50, "Building an Information Technology Security Awareness and Training Program," October 2003 and 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," April 1998. NIST 800-50 was more appropriate for our review of specialized training than NIST 800-16 because it focuses on a higher strategic level that better reflects the state of the DoD training program. According to NIST 800-50, agency Chief Information Officers should establish an overall strategy for the IT security awareness and training program; ensure that the agency head, senior managers, and others understand the concepts and strategies of the security awareness and training program and are informed of the progress of the program's implementation; and ensure that effective tracking and reporting mechanisms are in place.

NIST 800-50 describes the four phases of a training program: the program design, awareness and training material development, the program implementation, and postimplementation. The very first step in the design phase is determining the program structure. Organizations, such as DoD, that are relatively large, spread over a wide geographic area, and have organizational units

with separate and distinct missions often use a fully decentralized structure. In a fully decentralized program, a central authority, such as the DoD CIO, sets the overall training policy, and the operating units, such as the DoD Components, develop specific training plans and report the accomplishment of those plans to the central authority. In addition, NIST 800-50 endorses using a central database in the postimplementation phase. Agency CIO's could use the information in the central database to inform the agency head and other senior management officials of the compliance of the IT security awareness and training program, and agency auditors could use it to monitor compliance with security directives and agency policy. For more information on NIST 800-50 and 800-16, see Appendix B.

Implementation of DoD Guidance

DoD guidance since 1998 has acknowledged a need to identify personnel performing information assurance (IA) and IT duties, to develop training and certification requirements for those people, and to implement a process for tracking implementation of those requirements. A memorandum issued in June 1998 required each DoD Component to develop a training and certification plan within 45 days, report to the DoD CIO on the implementation of that plan every quarter, and fully implement the plan by December 2000. In August 1999, an IA and IT human resources integrated process team issued a report on DoD training, certification, and personnel management. The report included recommendations to identify IT personnel, establish training and certification programs, and track implementation of those programs. A Deputy Secretary of Defense memorandum, issued in July 2000, endorsed the integrated process team recommendations, assigned recommendations to specific organizations requiring them to develop and submit implementation plans within 90 days, and required the DoD CIO to provide a consolidated status report on execution of those plans every 60 days.

DoD Instruction 8500.2, "Information Assurance (IA) Implementation," issued on February 6, 2003, did not fix the problems or implement the requirements of either the June 1998 memorandum or the July 2000 memorandum. Instruction 8500.2 reiterated the need for a DoD core curriculum for IA training and awareness and an IA skills certification standard. In addition, it required the DoD Components to follow the June 1998 and July 2000 memorandums, even though those memorandums outlined specific timelines for implementing corrective actions that should have been completed prior to issuance of DoD Instruction 8500.2. DoD Directive 8500.1, "Information Assurance," issued on October 24, 2002, and certified current as of November 21, 2003, also required the DoD CIO to develop and promulgate additional IA policy and guidance on IA training and education.

On August 15, 2004, DoD issued DoD Directive 8570.1, "Information Assurance Training, Certification and Workforce Management." DoD Directive 8570.1 outlined roles and responsibilities that are consistent with a fully decentralized organization as defined in NIST 800-50; however, similar requirements have existed in other policy documents for years and have yet to be implemented. DoD policies are described in more detail in Appendix C. Better metrics, timelines, reporting mechanisms, and oversight are needed to enforce all of the requirements

in DoD Directive 8570.1. An implementing manual for DoD Directive 8570.1 is being staffed and is expected to be released in April 2005. Until the implementing manual is issued and complied with, DoD needs to report its training deficiencies under the Federal Managers Financial Integrity Act (FMFIA), as discussed later in this finding.

Review of Selected DoD Component Training Programs

Because DoD did not use an enterprisewide system, database, or process to identify employees performing significant IT security responsibilities and to track the specialized training taken by those employees, we selected 3 of the 21 DoD Components, the Defense Commissary Agency (DeCA), the Defense Contract Management Agency (DCMA), and the Washington Headquarters Service (WHS) that reported on specialized training for employees with significant IT security responsibilities in the DoD FY 2003 FISMA report for our review.

Identification of Employees with Significant IT Security Responsibilities. One of the most significant findings in the IA and IT human resources integrated process team August 1999 report was that DoD was unable to expeditiously determine who was performing IT activities and who had access to the DoD information infrastructure. The integrated process team recommended that DoD identify all people who perform IT functions in DoD personnel databases so that their training can be tracked. On July 14, 2000, the Deputy Secretary of Defense endorsed the integrated process team recommendation and required the Under Secretary of Defense for Personnel and Readiness to submit an implementation plan within 90 days. In the FY 2002 Performance and Accountability Report mandated by the FMFIA of 1982, DoD reported that it would develop the capability to identify and track IA and IT personnel in the civilian databases by June 2003 and in the military databases by June 2004.

The FY 2004 DoD FISMA reporting guidance issued by the DoD CIO on March 15, 2004, defined significant security responsibilities as those performed by Designated Approving Authorities, IA officers, IA managers, system administrators, computer emergency response team members, and anyone with privileged access to a system or network. As of May 2004, some DoD Components still were not using personnel databases to identify their employees with significant IT security responsibilities for FISMA reporting purposes. DeCA, DCMA, and WHS used data calls and the institutionalized knowledge of senior IT managers, rather than a personnel database, to identify their employees with significant IT security responsibilities. In addition, the number of IT employees that DCMA identified differed significantly from the number of employees that occupied IT-related positions in its personnel databases.

In FY 2003, DCMA reported that it had 98 employees with significant IT security responsibilities. In April 2004, the East and West DCMA Field Service Division Chiefs and DCMA headquarters personnel identified 199 IT security

professionals. In June 2004, the DCMA civilian personnel database contained 472 civilian employees who occupied traditional IT-related occupational series.[1]

Training and Certification Requirements. In June 1998, the DoD CIO and the Under Secretary of Defense for Personnel and Readiness issued a memorandum that acknowledged a need for better training of employees with significant IT security responsibilities. That memorandum required DoD Components to develop and implement certification plans within 45 days, to report on progress against those plans every quarter, and to fully implement those plans by December 2000. In July 2000, the Deputy Secretary of Defense assigned the Under Secretary of Defense for Personnel and Readiness with the responsibility for establishing a requirement for DoD Components to develop mandatory training or certification programs. Additionally, DoD Instruction 8500.2, issued in February 2003, required DoD Components to follow the June 1998 and July 2000 requirements. Although Component-level certification plans have been required since 1998, DoD did not develop mechanisms to ensure that DoD Components comply with these requirements. DeCA and DCMA did not have mandatory training or certification requirements for their employees with significant IT security responsibilities. WHS had specific training requirements for Designated Approving Authorities, IA officers, IA managers, and system administrators.

DeCA Requirements. DeCA was still developing a comprehensive training program with minimum training requirements for its employees with significant IT security responsibilities. Prior efforts to define training requirements either were not implemented or did not cover all IT security professionals. The DeCA "Information Assurance Training Plan for FYs 2001 and 2002" provided training requirements for system administrators only and was never fully implemented. According to DeCA officials, because their IA office had limited resources, they decided to focus on improving the system certification and accreditation status. In FY 2002, DeCA developed a training program for its IA officers that included three required classes and a database to track completion of those requirements. DeCA plans to modify the classes required for the IA officers. DeCA has been developing an IA Training Handbook since 2003. The handbook is the agency's best effort to date to develop and document training requirements for employees with significant IT security responsibilities; however, the handbook had not been completed and issued during our review of DeCA.

DCMA Requirements. DCMA did not have mandatory training and certification requirements for its employees with significant IT security responsibilities. Instead, DCMA used an IT Career Guide that provided information about the desired experience, education, and training goals for DCMA employees who perform IT as their primary function. The Career Guide has 3 career levels for the 10 specialty areas identified in the GS-2210 job series. Although the Career Guide provides a framework of recommended training for

[1] According to a study published in May 2004 by the Federal CIO Council's Committee on Workforce and Human Capital for IT, there are five traditional IT-related occupational series. They are GS-2210 Information Technology Management, GS-334 Computer Specialist (this series was canceled by the Office of Personnel and Management, but not all agencies have converted their Computer Specialists to other appropriate series), GS-391 Telecommunications, GS-1550 Computer Science, and GS-854 Computer Engineering.

each specialty and career level, DCMA representatives were unable to explain how the IT Career Guide is implemented. They could not describe processes for approving and documenting achievement of each career level. In addition to the IT Career Guide, DCMA was developing a certification program for systems administrators, which will focus on commercial certifications such as Microsoft, ORACLE, and CISCO.

WHS Requirements. WHS had specific training requirements for employees with significant IT security responsibilities that were primarily based upon requirements listed in appendixes of the June 1998 memorandum and WHS IA Bulletin 2001-002, "Organizational IA Training Resources," April 10, 2001; however, they were not formally documented. Designated Approving Authorities and IA managers must complete the "DAA, Designated Approving Authority" computer-based training provided by the Defense Information Security Agency. Level I system administrators must complete five specific training courses, pass a system administrator certification exam, and obtain supervisory validation of competency for the Level I tasks included in Appendix A of the June 1998 memorandum. Level II system administrators must complete two additional training courses and obtain supervisory validation of the Level II tasks. Level III system administrators must have additional formal training, knowledge of networking, fluency in one or more command languages, management or supervisory experience, and the ability to manage the budget, design the security architecture, and integrate security solutions. IA officers must take four of the five training courses required for Level I system administrators.

Tracking and Monitoring. Although the July 2000 Deputy Secretary of Defense memorandum specifically required the Under Secretary of Defense for Personnel and Readiness to require DoD Components to develop a capability to readily produce detailed answers about the status of certifications, only WHS had a process in place to identify and track training taken by employees with significant IT security responsibilities. DeCA and DCMA relied on data calls to provide training records for some or all of their IT security professionals.

DeCA Process. Prior to May 2004, DeCA did not have either a database or a central location for maintaining its training records. DeCA used a data call to provide training records in June 2004 for 128 employees with significant IT security responsibilities and recorded the results in an Excel spreadsheet. DeCA IT security professionals received very little training since 2001. According to the information that DeCA gathered from those employees, only 31 of 128 had taken IT-related training, other than the IA security awareness training, from January 2001 through June 2004. Of those 31, only 1 had taken more than two IT-related training courses.

DCMA Process. Although DCMA used different automated programs or databases for training, it did not have a central database of training and certification records that could be used to track and monitor training for its employees with significant IT security responsibilities. We requested training records for a judgmental sample of 25 employees with significant IT security responsibilities. DCMA forwarded our request to each of the individuals that we selected. Those employees submitted their training information to the DCMA training representative, who then consolidated the information and provided it to us. DCMA provided training records for 13 of the 25 employees that we selected.

Only 5 of the 13 employees with significant IT security responsibilities that provided training records had taken any IT-related training courses, other than IA security awareness training, since January 2001. Of those five, only two had taken more than two IT-related training courses.

WHS Process. WHS is implementing a software management tool to manage training for its employees with significant IT security responsibilities in two of its six Directorates. When demonstrated in May 2004, the program was capable of identifying the names of all employees in the two Directorates and displaying their individual training histories. The tracking and monitoring program will be extended to the other four Directorates, depending on its success in the first two directorates.

Training records for the four Directorates that are not using the software management tool are maintained by each Directorate IT Manager. Employees with significant IT security responsibilities are responsible for providing their IT Manager with appropriate documentation on completed training, and IT Managers are responsible for ensuring that their designated security personnel complete the appropriate IA training. WHS provided training records for a judgmental sample of the 25 employees that we chose. Based on the documentation WHS provided for the judgmental sample, employees received the training required by WHS for their position responsibilities.

Deficiency Reporting and Tracking

DoD has not consistently reported on training-related planned actions included in the FMFIA and FISMA reports. DoD reported two training-related corrective actions in the FY 2002 FMFIA report, but did not report on the progress in completing those actions in the FY 2003 FMFIA report. DoD also reported a training-related plan of action and milestones (POA&M) in its FY 2003 FISMA report, but the POA&M only addressed maintaining the currency of available training material and did not address specific weaknesses identified in the DoD FY 2002 FMFIA report or the August 1999 IA and IT human resources integrated process team report.

Federal Managers Financial Integrity Act. The FMFIA of 1982 (section 3512, title 31, United States Code) requires an annual assessment of and report on management controls. Specifically, section 2 of the FMFIA requires the head of each executive agency to annually report to the President and Congress on material weaknesses in the agency's controls and include a statement on whether there is reasonable assurance that the agency's controls are achieving their intended objectives. A material weakness is a deficiency that the agency head determines to be significant enough to be reported outside the agency. The report on material weaknesses must include agency plans and progress in correcting the material weaknesses. In addition, FISMA requires each agency to address the adequacy and effectiveness of information policies, procedures, and practices as part of the FMFIA review and to report any related significant deficiencies as a material weakness in the FMFIA report.

OMB Circular A-123, "Management Accountability and Control," June 21, 1995, provides implementing guidance for the FMFIA. It states that agency managers are responsible for taking timely and effective action to correct management control deficiencies and should be considered an agency priority. Plans should be developed to correct all material weaknesses, and progress against those plans should be periodically assessed and reported to agency management. A determination that a deficiency has been corrected should be made only when sufficient corrective actions have been taken and the desired results achieved. This determination should be in writing and available for review by appropriate officials.

In FY 2002, DoD reported information assurance as one of eight systemic weaknesses[2] and included two planned actions for specialized training of DoD employees performing significant IT security responsibilities. DoD stated that the DoD CIO would complete enterprisewide certification standards for IA and IT professionals by May 2003, and identify and track IA and IT civilian personnel in databases by June 2003 and in military personnel in databases by June 2004. DoD did not report on the progress of these actions in the FY 2003 FMFIA report signed on December 23, 2003, even though the DoD IA Strategic Plan released in January 2004 acknowledged a continuing need for completing certification standards and identifying IA and IT personnel in databases.

Plan of Action and Milestones. The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress in correcting security weaknesses found in programs and systems. OMB Memorandum 03-19 required agencies to develop POA&Ms for all programs and systems where an IT security weakness was found. Agency progress in correcting weaknesses in the POA&Ms must be reported to the OMB Director as part of FISMA.

In the FY 2003 FISMA report, DoD reported a POA&M for maintaining up-to-date training and stated that additional training material would be provided to DoD employees. The POA&M was incomplete because it did not address weaknesses and corrective actions discussed in either the FY 2002 FMFIA report or the 1999 IA and IT human resources integrated process team report. For example, it did not address either the DoD inability to identify and track employees with significant IT security responsibilities or the lack of training and certification requirements for those people. In addition, the POA&M did not provide estimated completion dates for the planned corrective actions. As a result, this weakness was closed in July 2004, even though serious IT training issues still exist.

FISMA Reporting

DoD reported unsupportable training information to OMB and Congress in September 2003 because the DoD did not have a definitive means to identify employees with significant IT security responsibilities or an enterprisewide

[2] DoD defines systemic weakness as those management control deficiencies that may affect a significant number of DoD Components and also have an adverse impact on the overall operations of DoD.

training standard and tracking mechanism. DeCA, DCMA, and WHS used data calls and the institutionalized knowledge of senior IT managers, rather than a personnel database, to identify their employees with significant IT security responsibilities. Therefore, the number of employees reported by DoD are subject to interpretation and change. For example, DeCA, DCMA, and WHS reported 21, 98, and 34 employees with significant IT security responsibilities during the FY 2003 FISMA reporting process, but identified 128, 199, and 76 employees with significant IT security responsibilities during our review.

In FY 2003, DoD reported that 7 of 21 DeCA employees with significant IT security responsibilities and 98 of 98 DCMA employees with significant IT security responsibilities received specialized training. However, neither DeCA nor DCMA could explain their criteria for determining whether their employees with significant IT security responsibilities had received adequate specialized training. Until DoD implements prior recommendations for developing minimum training and certification requirements and for identifying and tracking training of employees with significant IT security responsibilities, it will be unable to provide accurate and meaningful information on the training of those employees to OMB and Congress.

Recommendations, Management Comments, and Audit Response

A. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness:

1. Provide DoD Components with a standardized definition for employees with significant security responsibilities for information technology that require specialized training to use in meeting Federal Information Security Management Act requirements.

Management Comments. Management does not concur. The Director, Defense Information Assurance Program commented that the recommendation is no longer applicable because it has been completed. Employees with significant information technology security responsibilities are defined in Appendix AP1 of the Draft Manual DoD 8570.1-Manual and the DoD Federal Information Security Management Act Reporting Guidance for FY 2004, 15 March 2004.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, established that it is DoD policy that privileged users and information assurance managers shall be fully qualified, trained, and certified to DoD baseline requirements to perform their information assurance duties. Personnel performing information assurance privileged user or management functions, regardless of job series or military specialty, shall be appropriately identified in the DoD Component personnel databases. All information assurance personnel shall be identified, tracked, and managed so that information assurance positions

are staffed with personnel trained and certified by category, level, and function. All positions involved in the performance of information assurance functions shall be identified in appropriate manpower databases by category and level. The status of the DoD Component information assurance certification and training shall be monitored and reported as an element of mission readiness and as a management review item as stated in DoD Instruction 8500.2. DoD Directive 8570.1 specifically requires the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer to develop and promulgate additional guidance relating to information assurance training, certification, and workforce management requirements. Further, it directs that personnel and manpower databases under Under Secretary of Defense for Personnel and Readiness authority capture and report requirements for information assurance training and certification. As indicated in finding A, DoD guidance since 1998 has acknowledged a need to identify personnel performing information assurance and information technology duties, to develop training and certification requirements for those people, and to implement a process for tracking implementation of those requirements. This need cannot be met without defining the personnel to whom it pertains. An implementing manual for DoD Directive 8570.1 has not yet been issued; until such a manual is issued and complied with, this recommendation will not be completed. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

2. Establish a specific reporting process for reviewing and approving:

a. methodologies used by DoD Components to identify employees with significant information technology security responsibilities,

b. training and certification requirements developed by the DoD Components for their employees with significant information technology security responsibilities, and

c. tracking processes that DoD Components use to determine how many of their employees with significant security responsibilities for information technology have received specialized training.

Management Comments. The Director, Defense Information Assurance Program does not concur with this recommendation. US Code Title 10 assigns the Services specific responsibilities for equipping, training, and providing the forces. The Services review and provide oversight for their training programs. The Office of the Secretary of Defense provides the framework for the Components to address Recommendations a., b., and c. The Assistant Secretary of Defense for Networks and Information Integration has been working with Under Secretary of Defense of Personnel and Readiness to develop methodologies for DoD Components to identify information assurance positions, and manage and track employee training and certification requirements.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. See the audit response to management comments on Recommendation 1. In addition, DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management,"

August 15, 2004, directs that the Under Secretary of Defense of Personnel and Readiness shall establish oversight for approval and coordination of certification development and implementation, require that personnel and manpower databases under the Under Secretary of Defense of Personnel and Readiness authority capture and report requirements for information assurance training and certification, and require the head of the DoD Components to determine requirements for military and civilian manpower and contract support for privileged users and information assurance managers. These actions have not occurred. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense of Personnel and Readiness provide additional comments in response to the final report.

3. Continue to report necessary corrective actions, including the development of certification standards for employees with significant information technology security responsibilities and the process for identifying and tracking personnel who perform that function, to the Secretary of Defense for inclusion in the DoD Federal Managers Financial Integrity Act reports.

Management Comments. The Director, Defense Information Assurance Program does not concur with this recommendation, based on his response to Recommendations 1. and 2. The DoD Chief Information Officer will continue to provide updates on the progress of implementing the requirements of Draft DoD 8570.1-M.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. See the audit response to management comments on Recommendations 1. and 2. Further, in FY 2002, DoD stated that the DoD Chief Information Officer would complete enterprisewide certification standards for information assurance and information technology professionals by May 2003; identify and track information assurance and information technology civilian personnel in databases by June 2003; and identify and track information assurance and information technology military personnel in databases by June 2004, in accordance with the Federal Managers Financial Integrity Act of 1982. These actions have not occurred. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

4. Develop a Plan of Action and Milestones to address the significant deficiency in specialized training. The Plan of Action and Milestones should include Recommendations 1. and 2. as part of the planned actions needed to correct the overall significant deficiency and should include estimated completion dates for those planned actions.

Management Comments. Management does not concur. The Director, Defense Information Assurance Program commented that this recommendation is no longer applicable based on his response to Recommendations 1. and 2. The Director, Defense Information Assurance Program does not agree that DoD has a

significant weakness in specialized training, and stated that.findings A and B of the Office of the Inspector General report do not identify specialized training as a significant deficiency.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. See the audit response to management comments on Recommendations 1. and 2. Further, the DoD FY 2003 Federal Information Security Management Act report contained a Plan of Action and Milestone, which stated that additional training material would be provided to DoD employees; however, it was incomplete because it did not address weaknesses and corrective actions discussed in either the FY 2002 Federal Managers Financial Integrity Act report or the 1999 information assurance and information technology human resources integrated process team report. In addition, the Plan of Action and Milestone did not provide estimated completion dates for the planned corrective actions. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

5. Require DoD Components to specify in their data call responses to the Federal Information System Management Act:

a. the process used to identify employees with significant information technology security responsibilities,

b. the training requirements for employees with significant information technology security responsibilities, and

c. the process used to track and monitor compliance with those training requirements.

Management Comments. The Director, Defense Information Assurance Program, does not concur with this recommendation, and stated that this level of detail is not required in the E-Government Act and the Office of Management and Budget Federal Information Security Management Act guidance. DoD does report general training descriptions as part of the DoD response to the Office of Management and Budget's Federal Information Security Management Act reporting guidance.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. The E-Government Act of 2002 states that the National Institute of Standards and Technology shall have the mission of developing standards, guidelines, and minimum requirements for operating and providing security for information systems. National Institute of Standards and Technology 800-50 states that Chief Information Officers should establish overall strategy for the security awareness and training program and ensure that effective tracking and reporting processes are in place. A security awareness and training plan should include roles and responsibilities of personnel, and courses, material, and documentation of each aspect of the program. National Institute of Standards and Technology 800-50 also recommends the use of an automated tracking system to maintain information on program activity. National Institute of Standards and Technology 800-16 emphasizes a focus on roles and

responsibilities of an employee, as opposed to job titles, as a way of ensuring all employees receive proper training. DoD has neither adapted the National Institute of Standards and Technology guidance nor issued more stringent guidance to meet the requirements of the E-Government Act and should therefore determine the basis for DoD Component responses to the annual Federal Information Security Management Act data calls. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

6. Qualify the DoD annual Federal Information Security Management Act report to the Office of Management and Budget to acknowledge that the specialized training information provided has been self-reported by the DoD Components and that the DoD Chief Information Officer does not have enterprisewide standards, metrics, or tracking mechanisms with which to verify that information.

Management Comments. The Director, Defense Information Assurance Program does not concur with this recommendation, and stated that enterprise standards, metrics, and tracking mechanisms have been identified within DoD Directive 8570.1 and Draft DoD 8570.1-M.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. DoD Directive 8570.1 states that the DoD Chief Information Officer shall establish metrics to monitor and validate compliance with Directive 8570.1 as an element of mission readiness, but the Directive does not include what the metrics are. DoD Directive 8570.1 requires the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer to develop and promulgate additional guidance relating to information assurance training, certification, and workforce management requirements. Further, it directs that personnel and manpower databases under Under Secretary of Defense for Personnel and Readiness authority capture and report requirements for information assurance training and certification. As indicated in finding A, DoD guidance since 1998 has acknowledged a need to identify personnel performing information assurance and information technology duties, to develop training and certification requirements for those people, and to implement a process for tracking implementation of those requirements. An implementing manual for DoD Directive 8570.1 has not yet been issued. Until such a manual is issued and complied with, the DoD annual Federal Information Security Management Act report to the Office of Management and Budget and Congress should be appropriately qualified. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

7. Incorporate Recommendations 1. and 2. into the implementing manual for DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management."

Management Comments. Management does not concur. The Director, Defense Information Assurance Program commented that the Office of the Inspector

General Recommendation 7 is not applicable. Please see responses to Recommendations 1. and 2.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. Please refer to Audit Response to management comments on Recommendations 1. and 2. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

8. Provide direct assistance and oversight to the Chief Information Officers of the Defense Commissary Agency and Defense Contract Management Agency to improve their Component-level security programs for training and certifying employees with significant information technology security responsibilities until the DoD Chief Information Officer deems that the Component programs are adequate. If insufficient resources are available to provide such assistance and oversight, request immediate staff augmentation from the Secretary of Defense specifically for improving the DoD training program for DoD employees with significant security responsibilities for information technology.

Management Comments. The Director, Defense Information Assurance Program does not concur with this recommendation. As part of the implementation plan for the Draft DoD 8570.1-Manual requirements, the Defense Information Assurance Program is providing "start-up" sessions to ensure Component Chief Information Officers, human resources, and budget managers know and understand the requirements and are coordinating to meet them. Additionally, the Defense Information Assurance Program will have liaisons (Subject Matter Experts on implementing 8570.1-M) available on-call to the Components to support their initial implementation requirements.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. Please refer to audit response to management comments on Recommendations 1. and 2. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

B. Security Awareness Training

The DoD CIO did not ensure that security awareness training information that the DoD Components reported in response to FISMA data calls was accurate and supportable. Specifically, the DoD CIO did not ensure that the DoD Components had effective processes in place to track and monitor completion of security awareness training requirements. Although DeCA and WHS had processes in place to ensure that new employees receive initial security awareness training, WHS was the only agency of the three reviewed that had a process to ensure that their network users were receiving the required periodic training. This condition occurred because the DoD CIO had not established a specific reporting process to monitor and oversee DoD Components compliance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation." As a result, DoD security awareness training information reported in FY 2004 cannot be relied upon to accurately reflect DoD enterprisewide compliance with FISMA requirements, and network users that have not received training could introduce security vulnerabilities into DoD networks.

Federal Criteria

The Computer Security Act of 1987 established the initial requirement for periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information. Security awareness training enhances employees' awareness of the threats to and vulnerability of computer systems. OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," added a requirement for initial security awareness training before allowing individuals access to Federal computer systems. FISMA reinforced those requirements by requiring Federal agencies to develop, document, and implement an agencywide information security program. The programs must include security awareness training to inform all information system users, including contractors, of the information security risks associated with their activities and their responsibilities to comply with agency policies and procedures designed to reduce these risks.

OMB Memorandum 04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004, instructs Federal agencies to report the number of employees that they had in FY 2004 and how many of those employees received IT security awareness training in FY 2004, as described in NIST 800-50, "Building an Information Technology Security Awareness and Training Program," October 2003.

According to NIST 800-50, an effective IT security awareness and training program explains the proper rules of behavior for the use of agency IT systems and information, communicates IT security policies and procedures that need to be followed, reinforces good security practices, and teaches individuals to recognize IT security concerns and respond accordingly. NIST 800-50 lists 27 topics that could be addressed during awareness training, such as password usage,

viruses, Web usage policy, social engineering, incident response, changes in system environment, and security for handheld devices. Agency CIOs should establish overall strategy for the IT security awareness and training program; ensure that the agency head, senior managers, and others understand the concepts and strategies of the security awareness and training program and are informed of the progress of the program's implementation; and ensure that effective tracking and reporting mechanisms are in place. For more information on NIST 800-50, see Appendix B.

DoD Guidance

DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, requires all DoD employees and IT users to maintain a degree of understanding of IA policies and doctrine commensurate with their responsibilities. Each user should be capable of appropriately responding to and reporting suspicious activities and conditions and know how to protect the information that they access. To achieve this understanding, all DoD employees and IT users shall receive both initial and periodic IA security awareness training. DISA develops and provides awareness products, DoD Component Heads ensure that IA awareness training is provided to all military and civilian personnel, including contractors, and the DoD CIO provides oversight of DoD IA awareness activities.

Although not in effect at the time of our reviews of DeCA, DCMA, and WHS, DoD issued additional guidance on security awareness training. DoD Directive 8570.1, "IA Training, Certification, and Workforce Management," August 15, 2004, has similar requirements to DoD Instruction 8500.2, but strengthens the DoD awareness program by specifying that all IT users shall receive annual security awareness training rather than periodic training.

Initial Security Awareness Training.

DeCA and WHS both had processes in place to ensure that new employees receive initial security awareness training. They both provided new users with access to the network for a limited time for them to be able to complete the initial security awareness training. If the training was not completed during that time, network access was revoked. DCMA required new users to take initial security awareness training, but did not have a process to ensure that they took the training.

DeCA Initial Security Awareness Training. DeCA implemented an initial security awareness training program in the fall of 2003. Each new user is granted access to the network for 10 days. Users must complete the initial security awareness training and provide their certificates to their supervisors who forward to them to the Network Access Administrator. After they receive the certificates, new users will be granted permanent access to the network. If a training certificate is not forwarded to the Network Access Administrator within 10 days, the new user's network account will automatically expire.

DCMA Initial Security Awareness Training. DCMA made initial security awareness training available to new users on a continual basis. The training was included on a list of mandatory training courses on the DCMA Website. Users must provide their training certificates to their training coordinator upon completion; however, there was limited oversight within DCMA to ensure that new users complied with that requirement.

WHS Initial Security Awareness Training. WHS required all new employees to take initial security awareness training. New employees were granted 24-hour access to the network after receiving a security briefing from their IA Officer. If the new employee did not complete and pass the security awareness training within 24 hours, their user access was automatically revoked.

Periodic Security Awareness Training

The effectiveness of security awareness training varied among DoD Components. For example, DeCA and DCMA did not know how many of their employees with network access had received periodic security awareness training because they did not track and monitor completion of the training. Additionally, DeCA and DCMA could not provide supporting documentation for the information they provided for FISMA in FY 2003. In contrast, WHS was able to verify that all employees had completed security awareness training by comparing personnel records against security awareness training records.

DeCA. Although DeCA made security awareness training available to its employees by putting the training course on the intranet in January 2003, DeCA did not formally require periodic security awareness training until May 2004. On May 5, 2004, an e-mail informed all DeCA employees that security awareness training would be required annually and that all employees with network access were to take the training by May 21, 2004. DeCA uses the DISA "DoD Information Assurance Awareness" training CD, which is on the DeCA Website and is accessible to all DeCA employees with network access.

DeCA Tracking and Monitoring Efforts. Prior to May 2004, DeCA did not have a Componentwide process to track and monitor personnel who completed security awareness training. When employees completed the training, they printed out a blank certificate, wrote in their name, dated and signed the certificate, and provided it to their supervisor. DeCA did not have a central location where all of the certificates were maintained or a database to document which employees had taken training. During the audit, DeCA compiled security awareness training records through a data call to its four regions and recorded that information in an Excel spreadsheet. The training records provide DeCA with a rough estimate of how many people have taken the training, but it is not the best way to track and monitor completion of security awareness training. For example, DeCA cannot identify specific people who have not taken the training or ensure that all DeCA employees have responded to the data call unless a comparison against a personnel roster or list of network users is conducted. Such a comparison would be time-consuming unless it is integrated with the database or spreadsheet used to document the security awareness training completion

records. DeCA plans to incorporate the security awareness course into its Center for Learning's ToolBook, which will automatically track who completes the training.

DeCA Security Awareness Training Records. DeCA provided the Excel spreadsheet that contained completion dates for the security awareness training, as reported by the employees, for training completed from August 1, 2002, through May 31, 2004. Although DoD reported that all 17,876 DeCA employees received security awareness training in FY 2003, DeCA did not have accurate records on exactly how many employees completed the training during FY 2003. DeCA made security awareness training available to employees during 2003, but it did not keep records on the completion of that training until 2004. Based upon the records provided by DeCA as of May 31, 2004, only 5,322 employees had completed security awareness training in FY 2004. Many DeCA employees, such as those that work in the commissaries, do not have network access and therefore are not required to take the security awareness training, but DeCA did not have a process to identify those employees that had network access and whether they had received the required security awareness training.

DCMA. DCMA required all employees, including contractors, to take security awareness training every fiscal year. An e-mail is sent out every year to all DCMA employees to inform them of the annual security awareness training requirement. For example, DCMA sent out an e-mail on October 3, 2003, requiring all employees to complete the training by November 14, 2003. DCMA uses the Computer Security Awareness Training program, which is accessible through the DCMA intranet home page, to accomplish security awareness training. DCMA updates the security awareness training program around the beginning of every fiscal year, so that employees are not taking the same training each year.

DCMA Tracking and Monitoring Efforts. The Computer Security Awareness Training program includes a database that is updated every time a DCMA employee completes the security awareness training. The database included names of employees that had completed the training and the date that they completed the training. However, the database could not be used to quickly identify those who had not taken the training because it only included employees that had completed the training, rather than all DCMA employees. DCMA periodically checks agencywide compliance with its security awareness training requirements by comparing the total number of records in the Computer Security Awareness Training database against the number of DCMA employees reported by the personnel office. However, DCMA did not take any action if the number of records in the Computer Security Awareness Training database was less than the total number of DCMA employees.

DCMA Security Awareness Training Records. DCMA did not have supporting documentation for the security awareness training information provided in FY 2003. Officials were only able to provide records from their Computer Security Awareness Training database for security awareness training completed from September 10, 2003, through May 5, 2004. Although DoD reported that all 11,127 DCMA employees received security awareness training in FY 2003, based upon the records provided by DCMA, only 25 employees

completed security awareness training in FY 2003. However, through May 5, 2004, the Computer Security Awareness Training database contained 10,599 records for security awareness training completed in FY 2004. Of those 10,599 records, 9,767 were for training completed between October 3, 2003, when they were notified to take the training, and November 14, 2003, the date by which they were required to complete the training. The Computer Security Awareness Training database provides DCMA with a rough estimate of how many people have taken the training. However, without a comparison to a personnel roster or list of network users, DCMA will not know the exact number of employees requiring and receiving security awareness training. For example, since the Computer Security Awareness Training database automatically creates a record every time someone completes the online training, it would inadvertently include employees who had taken the training, but had subsequently left the agency and employees who had taken the training more than once.

WHS. WHS required annual security awareness training for all WHS employees. Each of the six WHS directorates sends an e-mail every year to its employees to inform them of the training requirement and the completion date for their directorate. Employees complete security awareness training and testing on an intranet Web site maintained by the WHS CIO office. After reading the training material, employees must answer 12 of 16 multiple choice questions correctly. WHS is replacing its security awareness training program with the Learning Management System, which is a Web-based security awareness training program. The Financial Management Directorate and Information Technology Management Directorate began using the new training in the spring of 2004.

WHS Tracking and Monitoring. Each directorate performs periodic, compliance checks of personnel and training information to ensure that all WHS users receive the security awareness training before or shortly after their required training completion date. Each directorate IT manager obtains personnel records from the administrative officer to determine the universe of employees in the directorate and notifies the employees that they must take the training. When employees complete the training, the training program automatically sends an e-mail to the directorate IT manager. The IT manager populates an Excel spreadsheet with all the names received from the administrative officer and adds the date that each employee completed training. The IT manager is responsible for identifying and contacting anyone who has not taken the security awareness training.

WHS Security Awareness Training Records. DoD reported that in FY 2003 all 1,707 WHS employees had completed security awareness training. WHS provided us with their security awareness training records on May 20, 2004. WHS does not keep records on a fiscal year basis or maintain historical records of dates when employees previously completed security awareness training. However, WHS was able to provide records that showed that all 1,644 WHS employees had completed security awareness training, according to the requirements that each WHS directorate designated for its employees. WHS does have a process in place to track whether their employees complete training, and the IT managers contact employees when they are due to complete training.

FISMA Reporting

DoD reported unsupportable information to OMB and Congress in its FY 2003 FISMA report. DoD reported that all 17,876 DeCA employees, all 11,127 DCMA employees, and all 1,707 WHS employees had received IT security awareness training in FY 2003. DeCA and DCMA were unable to provide supporting documentation for those numbers. Further, they did not have a process in place to track and monitor completion of security awareness training that would allow them to report accurately for FY 2004. Until the DoD CIO requires all DoD Components to have acceptable methods for tracking, monitoring, and documenting completion of security awareness training requirements, DoD will be unable to provide accurate and meaningful information on its security awareness training to OMB and Congress.

Conclusion

Recent attacks against the DoD information infrastructure have heightened awareness of the importance of training as a critical component of protecting DoD information resources against modern day cyber attacks. The DoD warfighting capability and the security of its information infrastructure are at great risk from attacks by foreign intelligence organizations, cyber terrorists, and the incompetence's of some of its own users. The shared risk environment created by highly connected and interdependent DoD information systems makes it imperative that all individuals using, administering, and maintaining those systems understand the threats and the policies, procedures, and equipment designed to mitigate those threats. Network users that have not received security awareness training could introduce security vulnerabilities into DoD networks. If employees are not informed of applicable organizational policies and procedures, they cannot be expected to act effectively to secure computer resources.

Recommendations, Management Comments, and Audit Response

B. We recommend that Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness:

1. Require each DoD Component to provide a plan for how it will track and monitor completion of security awareness training for their network users.

Management Comments. Management does not concur. The Director, Defense Information Assurance Program commented that the recommendation is no longer applicable as it has been completed. Chapters 6, 7, and 8 of the Draft DoD 8570.1-M identify information assurance workforce identification, tracking, and reporting requirements.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. DoD Directive 8570.1 requires that all authorized users of DoD information systems shall receive initial information assurance awareness orientation as a condition of access and thereafter must complete annual information assurance refresher awareness. Further, the Directive specifies that the status of DoD Component information assurance certification and training shall be monitored and reported as an element of mission readiness and as a management review item. The Assistant Secretary of Defense for Networks and Information Integration is charged with the responsibility to establish metrics to monitor and validate compliance with the Directive as an element of mission readiness, and the Under Secretary of Defense for Personnel and Readiness is charged with establishing oversight for approval and coordination of certification development and implementation. An implementing manual for DoD Directive 8570.1 has not yet been issued; until such a manual is issued and complied with, this recommendation will not be completed. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

2. Periodically review supporting documentation to ensure that the Components' plans are effectively implemented and to document completion of those reviews.

Management Comments. The Director, Defense Information Assurance Program does not concur with this recommendation, and stated that there is no requirement to perform Component inspections. However, DoD-wide standards, processes and procedures will be in place to support DoD management of these requirements. Additionally, the Defense Information Assurance Program is working with Components as they develop their plans to implement the requirements of DoD 8570 and will provide implementation support.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. National Institute of Standards and Technology 800-50 states that when a security awareness and training program is implemented, processes must be put in place to monitor compliance and effectiveness. DoD Directive 8570.1 requires that all authorized users of DoD information systems shall receive initial information assurance awareness orientation as a condition of access and thereafter must complete annual information assurance refresher awareness. Further, the Directive specifies that the status of DoD component information assurance certification and training shall be monitored and reported as an element of mission readiness and as a management review item. The Assistant Secretary of Defense for Networks and Information Integration is charged with responsibility to establish metrics to monitor and validate compliance with the Directive as an element of mission readiness, and the Under Secretary of Defense for Personnel and Readiness is charged with establishing oversight for approval and coordination of certification development and implementation. An implementing manual for DoD Directive 8570.1 has not yet been issued; until such a manual is issued and complied with, this recommendation will not be completed. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD

Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

3. Develop a Plan of Action and Milestones to address the security awareness training weakness. The Plan of Action and Milestones should include Recommendations 1. and 2. as part of the planned actions needed to correct the overall weakness and should include estimated completion dates for those planned actions.

Management Comments. The Director, Defense Information Assurance Program does not concur that DoD has a security awareness training weakness that requires a Plan of Action and Milestones at the enterprise level. The Director stated that the limited scope of the audit is not sufficient to support this conclusion.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. The scope of the audit included Federal laws, Office of Management and Budget guidance, National Institute of Standards and Technology guidance, and DoD Directives, Instructions, and Memorandums to determine the root cause of compliance deficiencies with these criteria at three DoD Components who reported 100 percent compliance with security training and awareness data calls in FY 2003. See also our response to management comments on Recommendations 1. and 2. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

4. Qualify its annual Federal Information Security Management Act report to the Office of Management and Budget to acknowledge that the security awareness training information provided has been self-reported by the DoD Components and the DoD Chief Information Officer does not have enterprisewide standards, metrics, or tracking mechanisms with which to verify that information.

Management Comments. The Director, Defense Information Assurance Program does not concur with this recommendation. The Director stated that enterprise standards, metrics, and tracking mechanisms have been identified within DoD Directive 8570.1 and Draft DoD 8570.1-M.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. DoD Directive 8570.1 requires that all authorized users of DoD information systems shall receive initial information assurance awareness orientation as a condition of access and thereafter must complete annual information assurance refresher awareness. Further, the Directive specifies that the status of DoD Component information assurance certification and training shall be monitored and reported as an element of mission readiness and as a management review item. The Assistant Secretary of Defense for Networks and Information Integration is charged with the responsibility to establish metrics to monitor and validate compliance with the Directive as an element of mission readiness, and the Under Secretary of Defense for Personnel and Readiness is charged with establishing oversight for approval and coordination of certification development and implementation. An implementing

manual for DoD Directive 8570.1 has not yet been issued. Until such a manual is issued, and complied with, the DoD annual Federal Information Security Management Act report to the Office of Management and Budget and Congress should be appropriately qualified. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

5. Provide direct assistance and oversight to the Chief Information Officers of the Defense Commissary Agency and Defense Contract Management Agency to improve their Component-level security programs for security awareness training until the DoD Chief Information Officer deems that the Component programs are adequate. If insufficient resources are available to provide such assistance and oversight, request immediate staff augmentation from the Secretary of Defense specifically for improving the DoD security awareness program.

Management Comments. The Director, Defense Information Assurance Program does not concur with this recommendation. As part of the implementation plan for the Draft DoD 8570.1-M requirements, the Defense Information Assurance Program is providing "start-up" sessions to ensure Component Chief Information Officers, human resources, and budget managers know and understand the requirements and are coordinating to meet them. Additionally, the Defense Information Assurance Program will have liaisons (Subject Matter Experts on implementing 8570.1-M) available on-call to the Components to support their initial implementation requirements.

Audit Response. The Director, Defense Information Assurance Program comments are nonresponsive. Please refer to our response to management comments on Recommendation 1. We request that both the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer and the Under Secretary of Defense for Personnel and Readiness provide additional comments in response to the final report.

Appendix A. Scope and Methodology

We performed this audit to determine whether all agency employees with computer access received IT security awareness training, and whether employees with significant IT security responsibilities received specialized IT training within our review of three DoD Components.

We reviewed Federal laws, OMB guidance, NIST guidance, and DoD Directives, Instructions and Memorandums. We reviewed DeCA, DCMA, and WHS training guidance, based on the size of the agencies and their geographic locations. We reviewed the lists of all personnel requiring security awareness training and employees with significant IT security responsibilities requiring specialized training. We also obtained and reviewed the records of security awareness training and IT specialized training to determine whether DeCA, DCMA, and WHS employees. were being trained in accordance with Federal laws, OMB guidance, DoD guidance, and their own internal guidance.

We visited, contacted, and conducted interviews with officials from the Office of the DoD CIO, DeCA, DCMA, and WHS.

We performed this audit from April 2004 through October 2004 in accordance with generally accepted government auditing standards.

We did not evaluate management controls because DoD recognized information assurance as a material weakness in the FY 2000 Statement of Assurance.

Use of Computer-Processed Data. We used each Component's Defense Civilian Personnel Data System roster to locate the five traditional IT-related occupations and compared them to the number of employees with significant IT security responsibilities that DeCA, DCMA, and WHS had provided. We did not perform a reliability assessment of the computer-processed data, although we did identify a coding and script error and a reversed month and date in a certain period, during our testing of the number of employees that had security awareness training by using Computer Security Awareness Training for DCMA. After the review detected the problem, DCMA took corrective action.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the Information Security high-risk area.

Prior Coverage

During the last 5 years, the Inspector General of the Department of Defense (IG DoD) and Naval Audit Service have issued three reports discussing computer security awareness training.

IG DoD

IG DoD Report No. D-2004-067, "Implementation of the Federal Information Security Management Act for FY 2003 at Selected Military Treatment Facilities," April 8, 2004

Naval Audit Service

N2004-0072, "Information Security – Operational Controls at Naval Air Systems Command Headquarters and Naval Air Warfare Centers," August 16, 2004

N2004-0063, "Information Security – Operational Controls at Naval Aviation Depots," July 9, 2004

Appendix B. National Institute of Standards and Technology Guidance on Security Awareness and Training

The Computer Security Act of 1987 tasked NIST to develop and issue guidelines for Federal computer security training. NIST issued Special Publication 500-172, "Computer Security Training Guidelines," in November 1989. In January 1992, the Office of Personnel and Management released a Federal personnel regulation, "Employees Responsible for the Management or Use of Federal Computer Systems," which required Federal agencies to provide training as set forth in NIST guidelines. In April 1998, the NIST 500-172 was superseded by NIST 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model." In October 2003, NIST 800-50, "Building an Information Technology Security Awareness and Training Program," was issued as a companion document to NIST 800-16. NIST 800-50 describes strategies for building an IT security awareness and training program, and NIST 800-16 describes a tactical approach to role-based IT security training.

NIST 800-50. NIST 800-50 provides guidance for building an effective IT security awareness and training program and supports the requirements specified in FISMA. Training agency IT users on security policy, procedures, and techniques is an important part of any IT security program. Agency heads must give high priority to effective security awareness and training for the workforce. CIO's should establish overall strategy for the IT security awareness and training program and ensure that effective tracking and reporting processes are in place. A security awareness and training plan should discuss existing policy and the scope of the awareness and training program. The plan should also include the roles and responsibilities of agency personnel; mandatory and optional courses or material; and documentation, feedback, and evidence of learning for each aspect of the program. The security training and awareness plan must be viewed as a set of minimum requirements to be met, and those requirements must be supportable from a budget or contractual perspective. An implementation schedule must be established and should consider availability of resources, organizational impact, and state of compliance.

NIST 800-50 outlines three possible program structures–centralized, partially decentralized, or fully decentralized program. A centralized program includes a central authority with the responsibility and budget for the entire organization's IT security awareness and training program. In a partially decentralized program, a central authority defines security awareness and training policy and strategy, and implementation, including budget allocation, material development, and scheduling is delegated to line management officials in the organization. In a fully decentralized program, the central authority disseminates broad policy and expectations for security awareness and training requirements, but gives responsibility for executing the entire program to other organizational units. This model normally uses a series of distributed authority directives, driven by the central authority, and a subsystem of CIOs and IT security program managers subordinate to the central CIO and IT security officer.

The central authority sets the overall policy, and the organizational units assess and develop the security awareness and training material and determine how to deploy it. The central authority may require periodic input from each organizational unit on the budget, strategy, and progress report. The central authority may also require the organizational units to report awareness and training results. Agencies that are relatively large, have general responsibilities assigned to headquarters, and specific responsibilities assigned to unit levels, have functions spread over a wide geographic area, or have quasi-autonomous organizational units with separate and distinct missions often use a fully decentralized structure.

When a security awareness and training program is implemented, processes must be put in place to monitor compliance and effectiveness. NIST 800-50 recommends the use of an automated tracking system to capture key information on program activity at an agency level. The database would serve the needs of several users. For example, CIO's could use the database to support strategic planning, report on overall implementation of the IT security awareness and training program, assist in security and IT budgeting, and identify the need for program improvements. The IT security program managers could use the database to support security planning, provide status reports, justify requests for funding, demonstrate compliance with agency-established goals and objectives, identify vendors and other training sources, and respond to security-related inquiries. Auditors could use the database to monitor compliance with security directives and agency policy. Other users that may have a need for the database include human resources departments, agency training departments, functional managers, and chief financial officers.

NIST 800-16. The emphasis of NIST 800-16 is on training criteria or standards, rather than on specific curricula or content. Training criteria should be based upon each employee's role within the organization and measured by on-the-job performance. This emphasis on roles and results, rather than on fixed content, gives this document flexibility, adaptability, and longevity. The new approach recognizes that an individual may have more than one organizational role and will need IT security training that satisfies the specific responsibilities of each role. In addition, because it is not focused on job titles, this approach facilitates more consistent interpretation of training criteria across organizations.

The NIST 800-16 is based on the premise that learning starts with awareness, builds to training, and evolves into education. This document defines the IT security learning needed as a person assumes different roles within an organization, different responsibilities in relation to IT systems, and the knowledges, skills, and abilities individuals need to perform the IT security responsibilities specific to their roles in the organization. All employees need awareness. Training is required for individuals whose role in the organization indicates a need for special knowledge of IT security threats, vulnerabilities, and safeguards. Education applies primarily to individuals who have made IT security their profession.

Appendix C. DoD Requirements

June 29, 1998, Memorandum. On June 29, 1998, the DoD CIO and the Under Secretary of Defense for Personnel and Readiness issued, "Information Assurance (IA) Training and Certification." This memorandum states that the shared risk environment created by highly connected and interdependent DoD information systems makes it imperative that all individuals using, administering, and maintaining shared systems understand the threats to DoD systems and the policies, procedures, and equipment designed to mitigate these threats. The memorandum also stated that many individuals using shared systems or performing the duties of system administrators and maintainers lacked sufficient training to ensure the adequate protection of DoD information resources.

The DoD CIO tasked the Under Secretary of Defense for Personnel and Readiness to work with the DoD Components to identify a common set of IA training and certification requirements for military and civilian occupational specialties. In the meantime, the memorandum required DoD Component Heads to develop and implement certification plans and procedures for all DoD military and civilian employees who use DoD computer systems or perform the duties of system administrators and maintainers. The certification plans were to be submitted to the Director of Information Assurance within the Office of the DoD CIO within 45 days, the Components were to report on progress against those plans every quarter, and the plans were to be fully implemented by December 2000.

July 14, 2000, Memorandum. On August 27, 1999, the Office of the Secretary of Defense published, "Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense," which included the findings and recommendations of an IA and IT human resources integrated process team composed of representatives from 15 DoD Services and agencies. The recommendations were accepted by the Deputy Secretary of Defense on July 14, 2000. The report found that DoD had difficulty determining who its employees with significant IT security responsibilities were because military and civilian employees who perform IT duties are not always assigned to a specific military or civilian IT occupational specialty or series. The report also found that DoD had not identified specific training and certification requirements for employees with significant IT security responsibilities. The report made 19 recommendations related to changing the way in which DoD manages its IT workforce. Recommendations to the Under Secretary of Defense for Personnel and Readiness included requiring the DoD Components to identify all people who perform IT functions in DoD personnel databases and to establish mandatory training or certification programs, or both, to track the status of compliance with the memorandum's requirements. The recommendation to adopt NIST 800-16 was directed to the DoD CIO.

On July 14, 2000, the Deputy Secretary of Defense issued a memorandum, "Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification and Personnel Management in the Department of Defense," which assigned actions to implement each of the 19 recommendations in the report. The memorandum

required the assigned organizations to develop and submit plans to implement their respective recommendation(s) to the Deputy Secretary's office within 90 days. The memorandum also required the DoD CIO to provide a consolidated status report on the execution of those plans every 60 days.

DoD Directive 8500.1. DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002, and certified current as of November 21, 2003, states that all personnel [with] authorized access to DoD information systems shall be adequately trained in accordance with DoD and Component policies and requirements and certified as required to perform the tasks associated with their IA responsibilities.

DoD Instruction 8500.2. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, states that the DoD CIO shall provide oversight of DoD IA education, training, and awareness activities. Specifically, the DoD CIO is responsible for establishing a DoD core curriculum for IA training and awareness and establishing IA skills certification standards in coordination with the Office of the Under Secretary of Defense for Personnel and Readiness. The DISA Director is required to develop and provide IA training and awareness products. DoD Component Heads are required to ensure that IA awareness, training, education, and professionalization are provided to all military and civilian personnel, including contractors, commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems in accordance with the DoD memorandums issued on IA training and certification on June 29, 1998, and July 14, 2000.

CJCS Instruction 6510.01C. Chairman of the Joint Chiefs of Staff Instruction 6510.01C, "Information Assurance and Computer Network Defense," May 1, 2001, states that all DoD Components will establish a training and certification program for Designated Approving Authority, Information System Security Officer, and system administrator positions using National Security Telecommunications and Information Systems Security national training standards. The Components are required to establish and maintain the certification status of system administrators. Certification information will be forwarded to DISA and documented in the DoD Central Database. The Components will also develop or use DISA-developed standardized tests for certification of skill level one, two, and three system administrators.

DoD Directive 8570.1. DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, states that the DoD CIO shall establish metrics to monitor and validate compliance with this Directive; DISA shall provide training and awareness materials for the DoD Components to integrate into their IA training and awareness programs; DoD Components shall "establish, resource, and implement" an IA training and certification program for all DoD Component personnel, and identify, document, and track IA personnel certification status in Component personnel databases; and the Under Secretary of Defense for Personnel and Readiness shall require Heads of DoD Components to determine the requirements for privileged users and IA managers, ensure that personnel databases capture and report IA training and certification requirements, and establish oversight for approving and coordinating development and implementation of certification programs.

DoD Directive 8570.1 duplicated several requirements that already existed in DoD guidance. DoD Instruction 8500.2, February 2003, already required the DoD CIO to provide overall oversight of the IA education, training, and awareness activities in DoD and required DISA to develop and promulgate IA training and awareness products. The June 1998 and July 2000 memorandums, as well as CJCSI 6510.01C, all required the DoD Components to develop IA training and certification requirements. The June 1998 memorandum already required the DoD Components to report to the DoD CIO on implementation of those requirements every quarter, the July 2000 memorandum required the DoD Components to identify their employees with significant IT security responsibilities and track compliance with training requirements in personnel databases, and CJCSI 6510.01C already required Components to forward certification information to DISA for inclusion in the DoD Central Database.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
Director, Program Analysis and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Information Systems Agency
Director, Defense Commissary Agency
Director, Defense Contract Management Agency
Director, Washington Headquarters Service

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Defense Information Assurance Program Comments

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NETWORKS AND INFORMATION INTEGRATION

23 NOV 2004

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Report on DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness (Project No. D2004AL-0136)

The Department of Defense (DoD) Deputy Chief Information Officer (DCIO) does not concur with findings A and B of the Report. The DCIO is concerned that the Report findings are based on an extremely limited sample of three relatively small DoD support Agencies (Defense Commissary Agency (DeCA), Defense Contract Management Agency (DCMA), Washington Headquarters Service (WHS)). The scope of the audit, which did not include any Services or Combatant Commands, represented less than 1% of total DoD employees and less than 0.2% of employees with significant IT security responsibilities. In contrast to the Report's conclusions, the results of the training audit revealed that WHS has a strong IT security training program.

The DCIO has completed action on two of the IG Report Recommendations and two Recommendations are not applicable. The DCIO does not concur with the remaining nine Recommendations of the subject Report. As requested, the following responses address the Report's Recommendations:

Part A: Specialized Training for Employees with Significant Security Responsibilities for Information Technology

OIG Recommendation 1: Provide DoD Components with a standardized definition for employees with significant security responsibilities for information technology that requires specialized training to use in meeting FISMA requirements.

DoD Management Response: OIG Recommendation 1 is no longer applicable as it has been completed. Employees with significant IT security responsibilities are defined in Appendix AP1 of the Draft Manual DoD 8570.1-M and in the *Department of Defense Federal Information Security Management Act (FISMA) Reporting Guidance for Fiscal Year 2004*, 15 March 2004. In accordance with the DoD FISMA guidance, page 2, DoD defines significant security responsibilities as those performed by the Designated Approval Authority (DAA), System Administrator/Network Administrator (SA/NA), Information System Security Manager (ISSM), Information Assurance Manager (IAM), Information System Security Officer (ISSO), Information Assurance Officer (IAO),

Computer Emergency Response Team (CERT) members, and anyone with privileged access to a system or network.

OIG Recommendation 2: In coordination with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), establish a specific reporting process for reviewing and approving:

a. methodologies used by DoD Components to identify employees with significant information technology security responsibilities.

b. training and certification requirements developed by the DoD Components for their employees with significant information technology security responsibilities, and

c. tracking processes that DoD Components use to determine how many of their employees with significant security responsibilities for IT have received specialized training.

DoD Management Response: The DCIO does not concur with this recommendation. United States Code Title 10 assigns specific responsibilities to the Services for equipping, training, and providing the forces. Under this responsibility, the Services are responsible for the review and oversight of their training programs. The Office of the Secretary of Defense (OSD) provides the framework for the Components to address recommendations a, b and c.

The Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) has been working directly with USD(P&R) to develop methodologies for DoD Components to identify IA positions and manage and track employee training and certification requirements.

OIG Recommendation 3: Continue to report necessary corrective action including the development of standards for employees with significant information technology security responsibilities and the process for identifying and tracking personnel who perform that function, to the Secretary of Defense for inclusion in the DoD Federal Managers Financial Integrity Act (FMFIA) report.

DoD Management Response: The DCIO does not concur with this recommendation based on DoD's Management Responses to OIG Recommendations 1 and 2. The DoD CIO will continue to provide updates on the progress of implementing the requirements of Draft DoD 8570.1-M.

OIG Recommendation 4: Develop a Plan of Action and Milestones to address the significant deficiency in specialized training. The POA&M should include Recommendations 1. and 2. as part of the planned actions needed to correct the overall significant deficiency and should include estimated completion dates for those planned actions.

DoD Management Response: This recommendation is no longer applicable based on DoD's Management Responses to OIG Recommendations 1, 2. The DCIO does not agree that DoD has a significant weakness in specialized training. Findings A and B of the OIG report do not identify specialized training as a significant deficiency.

OIG Recommendation 5: Require DoD Components to specify in their data call responses to the FISMA:

a. the process used to identify employees with significant information technology security responsibilities,
b. the training requirement for employees with significant information technology security responsibilities, and
c. the process used to track and monitor compliance with those training requirements.

DoD Management Response: The DCIO does not concur with this recommendation as this level of detail is not required in the E-Government Act and the FISMA guidance issued by the Office of Management and Budget (OMB). DoD does report general training descriptions as part of the Department's response to OMB's FISMA reporting guidance.

OIG Recommendation 6: Qualify its annual FISMA report to the OMB to acknowledge that the specialized training information provided has been self-reported by the Components and the DoD CIO does not have enterprise wide standards, metrics, or tracking mechanisms with which to verify that information.

DoD Management Response: The DCIO does not concur with this recommendation. Enterprise standards, metrics and tracking mechanisms have been identified within DoD Directive (DoDD) 8570.1, *Information Assurance Training, Certification and Workforce Management* and Draft DoD 8570.1-M.

OIG Recommendation 7: Incorporate Recommendations 1 and 2 into the implementing manual for DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management".

DoD Management Response: OIG Recommendation 7 is not applicable. Please see responses to Recommendations 1 and 2.

OIG Recommendation 8: Provide direct assistance and oversight to the CIOs of the Defense Commissary Agency and Defense Contract Management Agency to improve their Component-level security programs for training and certifying employees with significant information technology security responsibilities until the DoD CIO deems that the Component programs are adequate. If insufficient resources are available to provide

such assistance and oversight, request immediate staff augmentation form the Secretary of Defense specifically for improving the DoD training program for DoD employees with significant security responsibilities for information technology.

DoD Management Response: The DCIO does not concur with this recommendation. As part of the implementation plan for the Draft DoD 8570.1-M requirements, the DIAP is providing "start-up" sessions to ensure Component CIOs, human resources, and budget managers know and understand the requirements and are coordinating to meet them. Additionally, the DIAP will have liaisons (Subject Matter Experts on implementing 8570.1-M) available on-call to the Components to support their initial implementation requirements.

Part B: "Security Awareness Training"

OIG Recommendation 1: Require each DoD Component to provide a plan for how it will track and monitor completion of security awareness training for their network users.

DoD Management Response: OIG Recommendation 1 is no longer applicable as it has been completed. Chapters 6, 7, and 8 of the Draft DoD 8570.1-M identify IA workforce identification, tracking, and reporting requirements.

OIG Recommendation 2: Periodically review supporting documentation to ensure that the Component's plans are effectively implemented and to document completion of those reviews.

DoD Management Response: The DCIO does not concur with this recommendation as there is no requirement to perform Component inspections. However, DoD-wide standards, processes and procedures will be in place to support DoD management of these requirements. Additionally, the DIAP is working with Components as they develop their plans to implement the requirements of DoD 8570 and will provide implementation support.

OIG Recommendation 3: Develop a Plan of Action and Milestones to address the security awareness training weakness. The POA&M should include Recommendations 1. and 2. as part of the planned actions needed to correct the overall weakness and should included estimated completion dates for those planned actions.

DoD Management Response: The DCIO does not concur that DoD has a security awareness training weakness that requires a POA&M at the enterprise level. The limited scope of the audit is not sufficient to support this conclusion.

OIG Recommendation 4: Qualify its annual FISMA report to the OMB to acknowledge that the security awareness training information provided has been self-reported by the

Components and the DoD CIO does not have enterprise wide standards, metrics, or tracking mechanisms with which to verify that information.

DoD Management Response: The DCIO does not concur with this recommendation. Enterprise standards, metrics and tracking mechanisms have been identified within DoD Directive (DoDD) 8570.1, *Information Assurance Training, Certification and Workforce Management* and Draft DoD 8570.1-M.

OIG Recommendation 5: Provide direct assistance and oversight to the CIOs of the Defense Commissary Agency and Defense Contract Management Agency to improve their Component-level security programs for security awareness training until the DoD CIO deems that the Component programs are adequate. If insufficient resources are available to provide such assistance and oversight, request immediate staff augmentation form the Secretary of Defense specifically for improving the DoD training program for DoD employees with significant security responsibilities for information technology.

DoD Management Response: The DCIO does not concur with this recommendation. As part of the implementation plan for the Draft DoD 8570.1-M requirements, the DIAP is providing "start-up" sessions to ensure Component CIOs, human resources, and budget managers know and understand the requirements and are coordinating to meet them. Additionally, the DIAP will have liaisons (Subject Matter Experts on implementing 8570.1-M) available on-call to the Components to support their initial implementation requirements.

My point of contact for this action is George Bieber, 703-602-9980, george.bieber@osd.mil.

Robert G. Gorrie
Director, DIAP

5

Team Members

The Office of the Deputy Inspector General for Auditing of the Department of Defense, Acquisition and Technology Management prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Sarah Davis
James Mitchell
Kevin A. Palmer
Liyang Riggins
Kathryn Truex
Zachary Williams